Information Brokers and Privacy

DEREK J. SOMOGY*

ABSTRACT

The private sector has collected volumes of data on nearly all of us. Blending public and private data and analyzing it using clever algorithms has the potential to yield useful results, but is society willing to forego certain assumptions about what is private information in order to receive the benefits of the data? Is the public truly willing to miss out on those potential benefits for the sake of protecting what might already be public anyway? This article examines some of the most relevant events of 2005 concerning privacy and the commercial information industry.

I. INTRODUCTION

Information brokers came under great public scrutiny in 2005. The widely reported security breaches at ChoicePoint and LexisNexis, which focused attention on information-handling practices, heightened public concern over the security of personal information and have begun to shape the future of the data brokering market. At the same time, the information industry has continued to provide its services and assert the legality of its business methods. Indeed, federal and state legislative efforts emerged that attempted to address the concerns raised by privacy intrusions while recognizing the social benefits generated by the commercial information industry. This article presents significant events relating to the field of commercial information sellers and privacy that occurred in 2005, set against the contextual backdrop of the industry's evolving history. The topic is introduced by recounting the problems at ChoicePoint and LexisNexis. This article will sketch a brief evolution of the data industry, followed by critiques of the current regulatory frameworks and the industry's responses. The article concludes with a look at proposed federal legislation on the issue.

II. 2005 DATA BROKER PRIVACY CRISES – SECURITY BREACHES CALL ATTENTION TO THE INFORMATION BROKER INDUSTRY

In 2005, several high-profile security breaches magnified the attention that had already begun to focus on the personal data industry.

---

* The author is a J.D. candidate at The Ohio State University Moritz College of Law, class of 2007. He received a bachelor of arts degree in physics, *cum laude*, from the College of Wooster in 2002.

When personal identifying information was stolen from ChoicePoint and LexisNexis by hackers, the privacy implications were immediately apparent: information about consumers was not adequately guarded and may have fallen into the hands of unauthorized users. After further consideration, it became apparent that, the privacy considerations surrounding this industry extended beyond problems of theft and unauthorized use. Identity theft may be mundane compared to the enormous scope of individual information being amassed, analyzed, and sold by commercial data brokers.

A. CHOICEPOINT

The 2005 10-K Annual Report filed with the Securities and Exchange Commission lists ChoicePoint's business as a "provider of enhanced information services" to four major markets: Insurance Services, Business Services, Government Services, and Marketing Services.[1] Early in February 2005, ChoicePoint began notifying over 30,000 California residents that their personal information held by ChoicePoint was accessed by unauthorized users. The consumer data was accessed by hackers posing as ChoicePoint customers to further identity theft crimes. ChoicePoint's initial response was limited to notifying the affected consumers only in California because of that state's notification requirement obligating firms to notify consumers when security breaches occur.[2] By the end of February, ChoicePoint acknowledged that some 145,000 "consumers in all 50 states, the District of Columbia and three territories might have been affected by a breach of the company's credentialing process."[3] California authorities estimated that closer to 500,000 consumers were affected by this breach.[4] Olatunji Oluwatosin of Los Angeles is currently in a California prison for his role in the crime, which remains under investigation.[5] In the wake of this incident, ChoicePoint has publicly

---

[1] ChoicePoint Inc., Annual Report (Form 10-K) at 4 (Mar. 16, 2005).

[2] CAL. CIV. CODE §§ 1798.29 and 1798.82 – 1798.84 (West 2005) (California's Notice of Security Breach Statutes); California maintains a website that is committed exclusively to the state's privacy concerns, http://www.privacy.ca.gov.

[3] *ChoicePoint Vows to Tighten Controls*, N.Y. TIMES, Feb. 22, 2005, at C3.

[4] U.S. Senator Dianne Feinstein, *Protecting Privacy Has Become a Federal Concern*, (Mar. 5, 2005), http://feinstein.senate.gov/news-idtheft0305.html.

[5] David Coker, *Identity Data Thief Faces New Charges*, LA TIMES, Aug. 31, 2005 at C2.

promised changes, especially with regard to notifying victims. According to Carol A. DiBattiste, the company's Chief Credentialing, Compliance and Privacy Officer, ChoicePoint has "made fundamental changes in our products, processes and policies, including the adoption of one of the strictest consumer notification policies in the industry."[6]

B. LEXISNEXIS

In March, LexisNexis announced that personal data at one of its subsidiary companies, Seisint, had been accessed by unauthorized persons. According to the LexisNexis press release announcing its acquisition of Seisint,

> Seisint provides information products that allow business, financial services, legal and government customers to quickly and easily extract valuable knowledge from a vast array of data. Its products, including Accurint™ and Securint™, support customers in critical activities such as debt recovery, due diligence, fraud detection, identity verification, law enforcement, legal investigations, pre-employment screening, resident screening, and data supercomputing. Seisint's services and products are supported by integrating the Seisint Data Supercomputer technology and patent-pending data linking methods.[7]

In industry parlance, Seisint's business is "data mining." According to its initial estimates, the unauthorized users may have gained access to some 310,000 individuals' sensitive data, including social security numbers or driver's license numbers.[8] LexisNexis identified fifty-nine

---

[6] Press Release, ChoicePoint, ChoicePoint Notifies Consumers (Sept. 22, 2005), http://www.privacyatchoicepoint.com/news/statement_091605.html.

[7] Press Release, LexisNexis, LexisNexis Completes Acquisition of Seisint, Inc. (Sept. 1, 2004), http://www.lexisnexis.com/about/releases/0730.asp.

[8] Press Release, LexisNexis, LexisNexis Concludes Review of Data Search Activity, Identifying Additional Instances of Illegal Data Access (Apr. 12, 2005), http://www.lexisnexis.com/about/releases/0789.asp [hereinafter LexisNexis Concludes Review].

instances of misuse, coming primarily from unauthorized persons using IDs and passwords of legitimate Seisint customers.[9]

III. THE DATA INDUSTRY

The information industry generates noteworthy revenues. In 2004, LexisNexis brought in over $2.2 billion and ChoicePoint over $900 million.[10] Some estimates put the total worldwide revenue created by the information industry in 2004 at over $250 billion.[11] The high monetary value of this business underscores both the high demand for and the prevalent use of information products. The larger scope of the information "universe" goes beyond the concerns of this article, so the present discussion is limited to the markets typified by LexisNexis and ChoicePoint, which includes personal identifying data gleaned from public records as well as data consensually disclosed by individuals to proprietary entities.[12] The way in which the information may be bought, sold, and arranged into a commercial product is what makes the industry's practices implicate privacy concerns.

Generally, the development of the information industry has paralleled the development of the computer industry. During the 1970s, businesses began to digitize marketable information and store it in searchable databases. As computing speeds and storage capacities increased, the scope and amount of information digitized and sold also increased. Continued improvement in computer technologies have resulted in the size of today's databases being on the order of petabytes (or 10^{15} bytes).

In Robert O'Harrow, Jr.'s 2005 book, *No Place to Hide*, he argues "[w]here the data revolution meets the needs of national security, there

---

[9] *Id.*

[10] Press Release, Reed Elsevier, Reed Elsevier Announces 2004 Full Year Results (Apr. 2005), http://www.reed-elsevier.com/index.cfm?articleid=1278; Press Release, ChoicePoint, ChoicePoint Reports Record Annual Revenue and Earnings per Share (Jan. 26, 2005), http://www.choicepointinc.com/choicepoint/news.nsf/1e81a178107b63b18525687f005493a7/e865631fe8b8db3385256f94007b77cb?OpenDocument (last visited Dec. 20, 2005).

[11] Press Release, Outsell, Inc., SIIA and Outsell, Inc. Work Together to Raise the Profile of the Information Industry, (Apr. 13, 2005) http://www.outsellinc.com/where/press_releases/siia_and_outsell_work_together (last visited Jan. 29, 2006).

[12] FEDERAL TRADE COMMISSION, INDIVIDUAL REFERENCE SERVICES: A REPORT TO CONGRESS (Dec. 1997), http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm (last visited Jan. 10, 2006).

is . . . No Place to Hide."[13] O'Harrow details how the private sector has amassed voluminous digital records of individuals' interactions with the world. O'Harrow describes information products, mostly connected to the concept of identity, that use esoteric technologies to go far beyond the industry's stock in trade credit reports. Referring to the information they provide to the government, he regards ChoicePoint as "the world's largest private intelligence operation."[14] Because the nature of the business evolved away from the intended scope of the Fair Credit Reporting Act ("FCRA"), O'Harrow sees these businesses as operating in a markedly unregulated environment. During the late 90s, the industry responded to hints of forthcoming regulation by adopting a self-regulatory scheme.[15] Under the umbrella "Individual Reference Services Group" ("IRSG"), company representatives argued to the Federal Trade Commission ("FTC") that industry-established norms would be sufficient to satisfy privacy concerns.[16] O'Harrow views the IRSG as "a strong lobby opposed to heavy data regulation."[17] Coupled with the popular media coverage of the aforementioned breaches at LexisNexis and ChoicePoint, *No Place to Hide* cast the information industry in a questionable light and no doubt contributed to the public interest in the issue.

On the other side of the argument, Derek Smith's *Risk Revolution* largely defends the information industry's recent product offerings.[18] Smith bases his analysis of the information industry's practices in a modern context largely characterized by asymmetric threats.[19] According to Smith, the responsible use of information may mitigate risks and that is a good thing. To support this, Smith points out how technologies like link analytics[20] can be used to uncover the

---

[13] ROBERT O'HARROW, JR., NO PLACE TO HIDE (2005), cover.

[14] *Id.* at 156.

[15] *Id.* at 150.

[16] *See* FEDERAL TRADE COMMISSION, *supra* note 12.

[17] O'HARROW, *supra* note 13 at 150.

[18] DEREK V. SMITH, RISK REVOLUTION: THE THREATS FACING AMERICA & TECHNOLOGY'S PROMISE FOR A SAFER TOMORROW (2004). Mr. Smith is the CEO of ChoicePoint.

[19] *Id.* at 52-56.

[20] Smith explains link analytics as "software that is designed to examine public records and other database information to detect connections and non-obvious relationships that may exist

confederates of known criminals or terrorists.[21] Indeed, the degree of connectedness between the September 11th hijackers is alarming and the potential ability to uncover the entire lot of them based on any one individual's connection to other known terrorists is appealing. Further, Smith argues that anchoring identity to DNA information, and having that information available in electronic databases may serve various criminal law interests, including exonerating the wrongly convicted and averting serial recidivism.[22] Smith, however, makes the practical realization that information must be handled responsibly because "[w]e want a balance between privacy *and* risk reduction."[23]

The year 2005 seemed primed for a conflict between privacy and reasonable uses of information. The data industry was collecting vast amounts of data on our day-to-day lives and processing it for sale in largely unknown and unregulated ways. Alternatively, the information industry has developed analytical tools that yield highly desirable results.

IV. PRIVACY CRITIQUES

Even before the security breaches of 2005 attracted nationwide attention to the commercial data industry, privacy groups were chafing at the industry's practices and pressed the federal and state governments to pay more attention to the industry's attendant privacy issues. The most notable of these groups include the Electronic Privacy Information Center ("EPIC") and the Center for Democracy and Technology ("CDT"). According to its Web site, "EPIC is a public interest research center [that focuses] public attention on emerging civil liberties issues and [protects] privacy, the First Amendment, and constitutional values."[24] Similarly, CDT "works to

---

among individuals and/or organizations engaged in conspiracy or criminal activity. Typically, this information is scattered among the billions of documents and records (e.g., a change of address) generated in the course of daily life. Sometimes these connections are intentionally hidden links. Analytics is not, as often portrayed in the media, all-powerful, invasive spyware used to probe the details of the everyday lives of ordinary people." *Id.* at 66.

[21] *Id.* at 71-73.

[22] *Id.* at 123-25.

[23] *Id.* at 180 (emphasis in original).

[24] About EPIC, http://www.epic.org/epic/about.html (last visited Jan. 12, 2006).

promote democratic values and constitutional liberties in the digital age."[25]

In late 2004, EPIC filed a letter with the Federal Trade Commission urging the agency to investigate ChoicePoint, and other commercial data brokers, to determine their compliance with the FCRA, and the adequacy of current legislation in dealing with privacy issues surrounding the private industry collection of records.[26] In moving from products covered under the FCRA to products not covered under the FCRA, EPIC argued that ChoicePoint and other data brokers are skirting the mandates of the law.[27] Specifically, any unregulated data products present a risk of returning to the pre-FCRA era of reports plagued with "inaccurate, falsified, and irrelevant information."[28] EPIC further argued that federal case law supports the rule that data products derived from FCRA protected sources are also protected by the FCRA.[29] Alternatively, if these products are truly outside the reach of FCRA regulation, EPIC urged the FTC to identify the problems in the industry and work with Congress to expand the coverage of the Act.[30]

Following the disclosure by ChoicePoint about its security breach, EPIC sent a letter to ChoicePoint's Chief Operating Officer requesting that ChoicePoint tell consumers precisely what information was accessed by the hackers and disgorge the money earned by the sale of the data.[31]

By early March, the U.S. Senate Committee on Banking, Housing, and Urban Affairs held a hearing on "Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information" that touched on the issues raised by the ChoicePoint and

---

[25] About CDT, http://www.cdt.org/about/ (last visited Jan. 12, 2006).

[26] Letter from EPIC to the Federal Trade Commission on ChoicePoint and FCRA Databases (Dec. 16, 2004), *available at* http://www.epic.org/privacy/choicepoint/fcraltr12.16.04.html.

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] Letter from EPIC to ChoicePoint on FCRA (Feb. 18, 2005), *available at* http://www.epic.org/privacy/choicepoint/cpltr2.18.05.html.

LexisNexis crises.[32] Indeed, Senator Richard Shelby (R-AL) announced that one purpose of the hearing was "to gain insight into the state of industry compliance with the laws designed to protect personal financial information and to learn whether the current legal framework provides adequate protections and has kept pace with changes in the marketplace."[33] In addition, Senator Jon S. Corzine (D-NJ) contemplated legislation that would cede to the FTC the ability to regulate "non-financial third party data collectors."[34] In his brief testimony, Senator Patrick Leahy (D-VT) urged that "[c]onsumers should know who has their data, what it is being used for and how they can correct mistakes. They should also have notice, consistent with law enforcement considerations, so that they can protect themselves."[35] This hearing was indicative of the attention that was beginning to focus on the information industry and its practices.

Five days later, EPIC President Marc Rotenberg testified before the U.S. House of Representatives Committee on Energy and Commerce's Subcommittee on Commerce, Trade and Consumer Protection.[36] Rotenberg testified that ChoicePoint's business practices impose great costs on victims of identity theft, circumvent the FCRA, and that the FTC was failing to "aggressively pursue privacy

---

[32] U.S. Senate Committee on Banking, Housing, and Urban Affairs Hearing Detail http://banking.senate.gov/index.cfm?Fuseaction=Hearings.Detail&HearingID=142 (last visited Jan. 4, 2006). (This website of the U.S. Senate Committee on Banking, Housing and Urban Affairs provides the details of the hearing and the testimony given at those hearings).

[33] *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Hearing Before S. Comm. on Banking, Housing, and Urban Affairs*, 109th Cong. (2005) (statement of Sen. Richard Shelby, Member, Senate Comm. on Banking, Housing, and Urban Affairs).

[34] *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Hearing Before S. Comm. on Banking, Housing, and Urban Affairs*, 109th Cong. (2005) (statement of Sen. Jon S. Corzine, Member, Senate Comm. on Banking, Housing, and Urban Affairs).

[35] *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Hearing Before S. Comm. on Banking, Housing, and Urban Affairs*, 109th Cong. (2005) (statement of Sen. Patrick Leahy).

[36] *Consumer Privacy and ChoicePoint Data Theft: Hearing before the H. Subcomm. on Commerce, Trade and Consumer Protection, Comm. on Energy and Commerce*, 109th Congress (2005) (statement of Marc Rotenberg, President, EPIC), *available at* http://energycommerce.house.gov/108/Hearings/03152005hearing1455/Rotenberg.pdf.

protection."[37] In identifying potential legislative options to deal with the issue, Rotenberg advocated a system that closely adheres to already understood Fair Information Practices and referred to a potential framework of regulation.[38]

"A Model Regime of Privacy Protection v. 2.0" is a proposed legislative framework written by Daniel Solove, Associate Professor of Law at George Washington University Law School and Chris Hoofnagle, Director, Electronic Privacy Information Center, West Coast Office.[39] After identifying the limits of the Fair Credit Reporting Act and the Privacy Act of 1974 in regulating the commercial data broker industry, the authors articulate sixteen desirable legislative "mandates," including:

1. **Universal Notice:** "[t]o ensure meaningful access, opt-out, and other rights, there must be a way to provide people with notice about all of the companies collecting their information."[40] This flows from the fact that the public is largely unaware of the companies who collect personal identifying data, and any control the public might exercise of that data.[41]

2. **Meaningful Informed Consent:** "[t]here must be a way to ensure that consumers can exercise meaningful informed consent about the uses and dissemination of their personal information."[42] Current industry practices give consumers inconsistent control over the data they disclose. This

---

[37] *Id.* at 7.

[38] *Id.* at 10.

[39] Daniel J. Solove & Chris J. Hoofnagle, *A Model Regime of Privacy Protection (Version 2.0)*, GWU Legal Studies Research Paper No. 132 (Apr. 5, 2005), http://ssrn.com/abstract=699701.

[40] *Id.* at 10.

[41] *Id.*

[42] *Id.* at 11.

mandate would grant more control to consumers to decide when and how to share information.[43]

3. **One-Step Exercise of Rights:** "[t]o ensure the meaningful exercise of rights with regard to personal information, there must be a way to exercise these rights in an efficient and easy manner that is centralized."[44] Exercising control over how one's data is shared would be difficult if the consumer had to notify each and every company that deals with the information. For this reason, it makes more sense to have easy to handle and centralized administrative controls.[45]

4. **Individual Credit Management:** "[t]o ensure effective individual management of consumer reporting, there must be a way for individuals to have knowledge when entities attempt to access their credit records and have the ability to block such access."[46] This measure would frustrate attempts by identity thieves to obtain credit in their victim's name.[47]

5. **Access to and Accuracy of Personal Information:** "[t]here must be a way for individuals to ensure that their personal information maintained by various data brokers is maintained accurately and that it is not kept for an unreasonable amount of time."[48] Consumers whose data is being sold by information businesses should have access to their personal identifying data so it can be monitored for inaccuracies; this information should persist only for limited times.[49]

---

[43] *Id.*

[44] *Id.* at 11-12.

[45] Solove & Hoofnagle, *supra* note 39 at 11-12.

[46] *Id.* at 12-13.

[47] *Id.*

[48] *Id.* at 13.

[49] *Id.*

6. **Secure Identification:** "[t]here must be a way to prevent readily available pieces of personal information from being used as passwords to gain access to people's records and accounts."[50] Institutions who grant access to information based on readily ascertained data (like birthdates or social security numbers) unnecessarily put consumers at risk of identity theft.[51]

7. **Disclosure of Security Breaches:** "[t]here must be a way for individuals to learn about security breaches that result in the leakage or improper access of their personal data."[52] Consumers are unable to take protective steps when their data is compromised if the businesses responsible for the data fail to notify those affected.[53]

8. **Social Security Number Use Limitation:** "[t]here must be a way to reduce the use of social security numbers by private sector businesses."[54] This measure would push back the current trend of using the social security number as a general purpose identifier.[55]

9. **Access and Use Restrictions for Public Records:** "[t]here must be a way to regulate access and uses of public records that maximizes exposure of government activities and minimizes the disclosure of personal information about individuals."[56] Transparency in government is not particularly served by the wholesale disclosure of personal data, so restrictions should be imposed to frustrate efforts to

---

[50] *Id.* at 14.

[51] Solove & Hoofnagle, *supra* note 39 at 14.

[52] *Id.* at 14-15.

[53] *Id.*

[54] *Id.* at 15.

[55] *Id.*

[56] *Id.* at 16.

farm commercially valuable data from public records while maintaining the public oversight purpose of the records.[57]

10. **Curbing Excessive Uses of Background Checks:** "[t]here must be a way to limit the use of background checks to those jobs where there is a reasonable and justifiable need."[58] Background checks now cost so little that they are undertaken in situations that do not necessarily warrant a detailed look into another's life.[59]

11. **Private Investigators:** "[t]here must be a system that ensures greater accountability in the private investigator profession."[60] Private investigators are not regulated like public law enforcement officials, thus they pose a risk for abusing information tools.[61]

12. **Limiting Government Access to Business and Financial Records:** "[t]here must be a way to engage in electronic commerce and routine transactions without losing one's expectation of privacy in personal data."[62] The government is keen to avoid problems that inhere in actually collecting data, so they often purchase it from private sector businesses. However, consumers should not be forced to forfeit an expectation of privacy in the data simply because the government gathers the data from a third-party business.[63]

13. **Government Data Mining:** "[t]here must be a way to ensure that government data mining does not permit law

---

[57] Solove & Hoofnagle, *supra* note 39 at 16.

[58] *Id.* at 16-17.

[59] *Id.*

[60] *Id.* at 17.

[61] *Id.*

[62] *Id.* at 18.

[63] Solove & Hoofnagle, *supra* note 39 at 18.

enforcement to engage in dragnet searches for prospective crimes. Where data mining is employed, it should occur in as open a way as possible with adequate judicial oversight and public accountability."[64] Indiscriminate use of link analytic technologies to uncover webs of association runs contrary to our society's long established legal and normative distaste for dragnet searches.[65]

14. **Control of Government Maintenance of Personal Information:** "[t]here must be meaningful regulation limiting the collection of personal data, acceptable uses, accuracy, security, and retention of personal information by government agencies, especially since they are acquiring more and more data about individuals."[66] This point brings attention to the fact that the Privacy Act of 1974 might not be adequate to protect privacy in 2005.[67]

15. **Preserving the Innovative Role of the States:** "[t]he ability of states to innovate new approaches to privacy protections must be preserved."[68] Above and beyond federal legislation, this requirement contemplates the possibility that states will enact even more protective privacy laws.[69]

16. **Effective Enforcement of Privacy Rights:** "[t]here must be a way to ensure that privacy protections are enforced with meaningful sanctions as well as provide meaningful redress to victims."[70] As long as plaintiffs are required to prove actual damages for privacy violations, the judicial

---

[64] *Id.* at 18-19.

[65] *Id.*

[66] *Id.* at 19-20.

[67] *Id.*

[68] *Id.* at 20-21.

[69] Solove & Hoofnagle, *supra* note 39 at 20-21.

[70] *Id.* at 21.

> enforcement of federal privacy policies will be shortchanged. This provision would make it easier for victims to recover, as well as encourage prudent industry practices.[71]

The "Model Regime" is a work in progress. Its second version (v. 2.0) embraced many of the suggestions offered after the release of v. 1.1.[72] At the end of March, Chris Hoofnagle testified before the California Senate Banking, Finance, and Insurance Committee on data security.[73] In his testimony, Hoofnagle listed the alarming quantity of smaller data companies ChoicePoint has acquired since 1997.[74] By arguing that "the public does not fully understand how this information is gathered, used, and sold," he argued that ChoicePoint has given privacy considerations short shrift.[75] Hoofnagle concluded by advocating that the state legislature embrace several positions from his "Model Regime" paper, discussed *supra*.[76]

Although ChoicePoint announced in early March that it was exiting the "non-FCRA consumer-sensitive data markets,"[77] Solove and Hoofnagle promptly rejected this announcement as insufficient to cure the problems for eight reasons. First, ChoicePoint's reforms only limit the market behavior of ChoicePoint and therefore do not represent a total solution to the problem.[78] Second, the use of

---

[71] *Id.*

[72] *See id.* at 22-36 (commentary on the Model Regime).

[73] *After the Breach: How Secure and Accurate is Consumer Information Held by ChoicePoint and Other Data Aggregators?: Hearing Before the Senate Banking, Finance and Insurance Committee*, 2005 Leg. Sess. (Ca. 2005) (statement of Chris Jay Hoofnagle, Director, Electronic Privacy Information Center West Coast Office), *available at* http://www.epic.org/privacy/choicepoint/casban3.30.05.html.

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] ChoicePoint to Exit Non-FCRA, Consumer-Sensitive Data Markets (Mar. 4, 2005), http://www.privacyatchoicepoint.com/news/statement_030405.html [hereinafter ChoicePoint to Exit].

[78] Daniel Solove & Chris Hoofnagle, *ChoicePoint's Response to the Sale of Information to Criminals is Inadequate*, EPIC ChoicePoint, http://www.epic.org/privacy/choicepoint/#inadequate (last visited Dec. 20, 2005).

truncated social security numbers is only a minor hurdle to anyone actually intent on getting the full number because it could be found from other sources.[79] Third, studies show that as many as 90% of these records contain errors.[80] Fourth, consumers have no way to correct public information in the ChoicePoint reports.[81] Fifth, ChoicePoint has little reason to cater to the interests of individuals whose records it sells.[82] Sixth, ChoicePoint is only retreating from a portion of the market and will continue to sell sensitive personal information in other contexts, including consumer-driven transactions and to accredited corporate customers.[83] Seventh, the exception to this policy for antifraud purposes is too broad.[84] And finally, ChoicePoint will continue to sell the personal information to government law enforcement agencies.[85]

In June, the Center for Democracy and Technology urged Congress to "amend the Privacy Act [of 1974] to make it clear that it applies to government use of commercial data."[86] CDT argued that the requirements of the Privacy Act of 1974 would be triggered by combined government/private sector databases.[87]

In July, Chris Hoofnagle testified before the U.S. House of Representatives Committee on Energy and Commerce's Subcommittee on Commerce, Trade, and Consumer Protection to give commentary on the "Discussion Draft of Data Protection Legislation."[88] Hoofnagle

---

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] *Id.*

[83] *Id.*

[84] Solove & Hoofnagle, *supra* note 78.

[85] *Id.*

[86] Memorandum from CDT to Data Privacy and Integrity Advisory Comm., DHS on Recommended Policies for Use of Private Sector Data, (Jul. 18, 2005), *available at* http://www.cdt.org/testimony/20050718schwartz.pdf.

[87] *Id.*

[88] *Data Security: The Discussion Draft of Data Protection Legislation: Hearing before the H. Subcomm. on Commerce, Trade and Consumer Protection, Comm. on Energy and Commerce*, 109th Congress (2005) (statement of Chris Jay Hoofnagle, Director and Senior Counsel, EPIC

went beyond the problems at ChoicePoint, and stressed the widespread problem of personal data mismanagement.[89] Citing statistics compiled by the Privacy Rights Clearinghouse, Hoofnagle recounted that group's accounting of the "Chronology of Data Breaches Reported Since the ChoicePoint Incident."[90] According to their estimates, over 50 million identities have been compromised in the U.S. by a wide array of private and public entities, which Hoffnagle used to support the drastic need for Congress to legislate in the privacy/data arena.[91] As to the Discussion Draft's proposals, Hoofnagle offered the following comments:

- The Discussion Draft should contain credit freeze language, thereby allowing individuals to prevent unauthorized credit requests made by identity thieves.[92]

- Any legislation must go beyond simply making personal data more secure, and pay attention to privacy interests apart from database security.[93] Although bolstered security measures may prevent hackers from gaining access to personal information, it is the industry practices that allow collection and preservation of certain data that may violate privacy norms.

- Companies should employ audit trails to deter and detect misuse of information.[94]

West Coast Office), *available at* http://www.epic.org/privacy/choicepoint/datasec7.28.05.html [hereinafter *Discussion Draft of Data Protection Legislation*].

[89] *Id.*

[90] A Chronology of Data Breaches Reported Since the ChoicePoint Incident, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Dec. 20, 2005).

[91] *Id.*

[92] *Discussion Draft of Data Protection Legislation*, *supra* note 88.

[93] *Id.*

[94] *Id.*

- Data brokers should be audited by the Federal Trade Commission, and individuals should be able to check their dossiers at no charge.[95]

- The standard for triggering a business' duty to notify consumers of an intrusion should be whether there is a "reasonable risk or reasonable basis to believe that such access could lead to misuse of personal information."[96] Also, the scope of the legislation should encompass companies that "owns or possesses data," as opposed to California's "any company that owns or licenses data."[97]

- Enforcement of the law by the Federal Trade Commission is appropriate under its authority to address unfair and deceptive trade practices.[98] However, enforcement powers should also extend to state Attorneys General.[99]

- The best definition of a data broker is "a business entity which for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages, in whole or in part, in the practice of collecting, transmitting, or otherwise providing personally identifiable information on a nationwide basis on more than 5,000 individuals who are not the customers or employees of the business entity or affiliate."[100]

---

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] *Discussion Draft of Data Protection Legislation, supra* note 88.

[99] *Id.*

[100] *Id.*

- Blanket federal preemption is not desirable–leave the states some ability to regulate privacy matters.[101]

- Privacy legislation should not automatically end via a "sunset" provision, although the issue should be revisited occasionally by the legislature.[102]

- The Federal Trade Commission should receive the funds necessary to enforce the law effectively.[103]

By and large, Hoofnagle supported the Discussion Draft.

In early November, a large coalition of privacy and consumer advocates conveyed their concerns over legislative attempts to improve privacy laws in a letter to Senators Arlen Specter (R-PA) and Patrick Leahy (D-VT).[104] Signing the letter were representatives from: the Center for Digital Democracy, Electronic Privacy Information Center, Identity Theft Resource Center, National Consumers League, Privacy Journal, Privacy Times, World Privacy Forum, Consumer Action, Liberty Coalition, PrivacyActivism, Privacy Rights Clearinghouse, and U.S. Public Interest Research Group. Worried that proposed legislation focused on data security to the detriment of greater policy considerations of privacy and fairness, the letter urged that legislation include the following:

- Notice of security breaches in all instances.[105]

- "A broad definition of identity theft," to cover both actual and attempted fraud.[106]

---

[101] *Id.*

[102] *Id.*

[103] *Id.*

[104] Coalition Letter on Data Security Bills to Senate Committee on the Judiciary (Nov. 9, 2005), http://www.epic.org/privacy/choicepoint/datamarker11.09.05.html.

[105] *Id.*

[106] *Id.*

- A consumer-friendly freeze on access to credit.[107]
- "Limits on collection, use, and disclosure of social security numbers."[108]
- Preservation of state laws and law-making ability.[109]
- "Special measures to address commercial data brokers."[110]

The privacy critiques of the information industry not only addressed the particular information products offered, but also the regulatory framework that allowed such products to be developed in the first place. Indeed, privacy interest groups have offered suggestions on how personal identifying information could be better handled. The effect of public, interest group, and congressional pressures on the information industry remains to be seen.

V. INDUSTRY RESPONSES

After being caught with significant data breaches in early 2005, data brokers like ChoicePoint and LexisNexis had to defend publicly their own practices and the industry generally. In some cases, the companies promised to alter how they conduct their business.

In March, ChoicePoint elected to discontinue selling identity products to a sector of its market that seemed to pose a great risk for identity theft.[111] In a press release, ChoicePoint CEO Derek Smith cited the recent fraud activity and consumer response as motivating the business decision, which was estimated to lower 2005 revenues by $15-20 million.[112] To be sure, ChoicePoint was not getting out of the

---

[107] *Id.*

[108] *Id.*

[109] *Id.*

[110] Coalition Letter on Data Security Bills to Senate Committee on the Judiciary, *supra* note 104.

[111] ChoicePoint to Exit, *supra* note 77.

[112] *Id.*

sensitive personal information market entirely but rather limited its future sales to three potential scenarios:[113]

1. "Support consumer-driven transactions where the data is needed to complete or maintain relationships such as insurance, employment and tenant screening or to provide access to their own data;"[114]

2. "Provide authentication or fraud prevention tools to large, accredited corporate customers where consumers have existing relationships. For example, information tools for identity verification, customer enrollment and insurance claims;"[115] or

3. "Assist federal, state and local government and criminal justice agencies in their important missions."[116]

4. In addition to immediately abandoning this market, ChoicePoint provided approximately $2 million in services to those consumers whose identities had been compromised.[117] Also, the company created "an independent office of Credentialing, Compliance and Privacy that will report to the Board of Directors' Privacy Committee."[118]

Like Hoofnagle, ChoicePoint also testified in front of the California Senate Banking, Finance, and Insurance Committee.[119]

---

[113] *Id.*

[114] *Id.*

[115] *Id.*

[116] *Id.*

[117] ChoicePoint, *supra* note 77.

[118] *Id.*

[119] *Hearing before the Senate Banking, Finance and Insurance Committee*, 2005 Leg. Sess. (Ca. 2005) (statement of Don McGuffey, Vice President, Data Acquisition and Strategy, ChoicePoint Services Inc.), *available at* http://www.epic.org/privacy/choicepoint/cp3.30.05.pdf.

After apologizing for the recent upsets caused by the company, ChoicePoint's Vice-President for Data Acquisition and Strategy, Don McGuffey, presented the Committee with a list of the beneficial services provided by ChoicePoint, including:

- "Identification and credential verification services to businesses, government, and non-profit organizations."[120]
- Identification of 11,000 undisclosed felons who were attempting to volunteer with youth organizations.[121]
- Law enforcement collaboration, including the identification of the D.C.-area snipers and providing services to the National Center for Missing and Exploited Children.[122]
- Helping American individuals and businesses obtain insurance products.[123]
- Facilitating employment through pre-employment background checks.[124]

As to regulation of the industry, McGuffey noted how the Fair Credit Reporting Act and the recently enacted Fair and Accurate Credit Transactions Act, the Gramm-Leach-Bliley Act, and the Drivers Privacy Protection Act all place limits on how ChoicePoint handles data.[125] Furthermore, he stated that ChoicePoint was committed to developing rigorous information security policies. To support this, he

---

[120] *Id.* at 2.

[121] *Id.*

[122] *Id.*

[123] *Id.*

[124] *Id.*

[125] *Hearings before the Senate Banking Committee, supra* note 119 at 3.

pointed to the recently created independent office of Credentialing, Compliance, and Privacy that reports to the Board of Directors' Privacy Committee, to be headed by a former senior prosecutor at the Justice Department with extensive experience in the detection and prosecution of financial fraud.[126] As was disclosed in March, McGuffey noted how ChoicePoint was abandoning a portion of the sensitive personal data market. He further apologized for the security breaches and pledged to support their victims.[127]

By the time LexisNexis announced its breach at Seisint in April, it had already notified the 30,000 individuals whose identities may have been accessed by unauthorized persons.[128] LexisNexis seems to have opted for a frank admission of the breach, which it discovered during its own internal investigation. To the victims of the breach, LexisNexis offered free support services, including credit reports, credit monitoring for one year, fraud insurance, and fraud counseling services.[129] According to its April press release, no individual who accepted the offer of free credit reports and monitoring had advised the company of "having experienced any form of identity theft."[130]

In addition to responding to the data breach crisis and testifying in front of legislators, ChoicePoint uses a website devoted to addressing privacy concerns, http://www.privacyatchoicepoint.com. In defense of its position and reputation, ChoicePoint has made the following postings:[131]

- **March 4, 2005:** ChoicePoint decided to exit the non-FCRA, consumer sensitive markets.[132]

---

[126] *Id.* at 4-5.

[127] *Id.* at 5-6.

[128] LexisNexis Concludes Review, *supra* note 8.

[129] *Id.*

[130] *Id.*

[131] Privacy at ChoicePoint: Company Statements, http://www.privacyatchoicepoint.com/news/statements.html (last visited Dec. 15, 2005).

[132] ChoicePoint to Exit, *supra* note 77.

- **May 4, 2005:** In response to an article in *The Wall Street Journal* claiming that the data breach covered "millions of people," ChoicePoint reasserted its estimate that "145,000 consumers may have had their personal information improperly accessed." Further, it stressed a commitment to fighting fraud and improving the quality of its business practices.[133]

- **July 12, 2005:** ChoicePoint posted the transcript of Carol DiBattiste's presentation to the Association of Certified Fraud Examiners. DiBattiste, ChoicePoint's Chief Credentialing, Compliance, and Privacy officer is a former Deputy Administrator of the U.S. Transportation Security Administration.[134]

- **August 23, 2005:** Contrary to claims in the press, ChoicePoint offered consumers the ability to see their own public records information at *no cost*.[135]

- **November 9, 2005:** To clarify an Associated Press story, ChoicePoint asserted that notifications disclosed in an SEC 10-Q filing do not represent previously undisclosed notices.[136]

VI. FEDERAL LEGISLATION

Members of Congress were concerned that current laws had not adequately regulated the commercial data broker industry, and several

---

[133] Press Release, ChoicePoint, ChoicePoint Responds to 5/3 Article in The Wall Street Journal, (May 4, 2005), http://www.privacyatchoicepoint.com/news/statement_050405.html.

[134] Press Release, ChoicePoint, Presentation to Association of Certified Fraud Examiners, (July 12, 2005), http://www.privacyatchoicepoint.com/news/statement_071205.html.

[135] Press Release, ChoicePoint, ChoicePoint Does Not Charge Consumers for Existing Information About Themselves, (Aug. 23, 2005), http://www.privacyatchoicepoint.com/news/statement_082305.html.

[136] Press Release, ChoicePoint, ChoicePoint Clarifies AP Story, (Nov. 9, 2005), http://www.privacyatchoicepoint.com/news/statement_110905.html.

bills appeared in the U.S. House and Senate during 2005. These included:

House Bill 3140, or the "Consumer Data Security and Notification Act of 2005."[137] This would amend the FCRA to bring data brokers within the Act's coverage. Also, the FTC would promulgate safeguards to protect non-public consumer information. The Gramm-Leach-Bliley Act would be amended to require security breach notifications. This bill was referred to the House Committee on Financial Services on June 30, 2005.

Senate Bill 500, or the "Information Protection and Security Act."[138] (Related to House Bill 1080). This would direct the FTC to promulgate regulations governing data brokers very close to the traditional Fair Information Practices. Violations would be treated as unfair or deceptive acts or practices under the Federal Trade Commission Act. States may bring civil actions. This bill was referred to the Committee on Commerce, Science, and Transportation on March 3, 2005.

Senate Bill 1789, "Personal Data Privacy and Security Act of 2005."[139] This would criminalize many of the acts that facilitate identity theft. Data brokers would be required to disclose personal records and have a mechanism in place for correcting inaccuracies. Further, the Act mandates that the Comptroller General investigate government use of commercial data products. This bill was placed on the Senate Legislative Calendar under General Orders, Calendar No. 297 on November 17, 2005.

VII. CONCLUSION

In 2005, there was a substantial shake-up of the information industry. Popular media coverage of the breaches at LexisNexis and ChoicePoint, books like *No Place to Hide*, and the actions of privacy interest groups all brought attention to the information industry's practices. The information industry responded by pointing out the

---

[137] Consumer Data Security and Notification Act of 2005, H.R. 3140, 109th Cong. (2005), *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d109:H.R.3140:@@@D&summ2=m&.

[138] Information Protection and Security Act, S. 500, 109th Cong. (2005), *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d109:S.500:@@@D&summ2=m&.

[139] Personal Data Privacy and Security Act of 2005, S. 1789, 109th Cong. (2005), *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d109:S.1789:@@@D&summ2=m&.

benefits of its technologically impressive products and attempting to avoid heavy regulation. Congress is interested in the issue and it seems possible that it will update privacy laws to bring them into the 21st century.